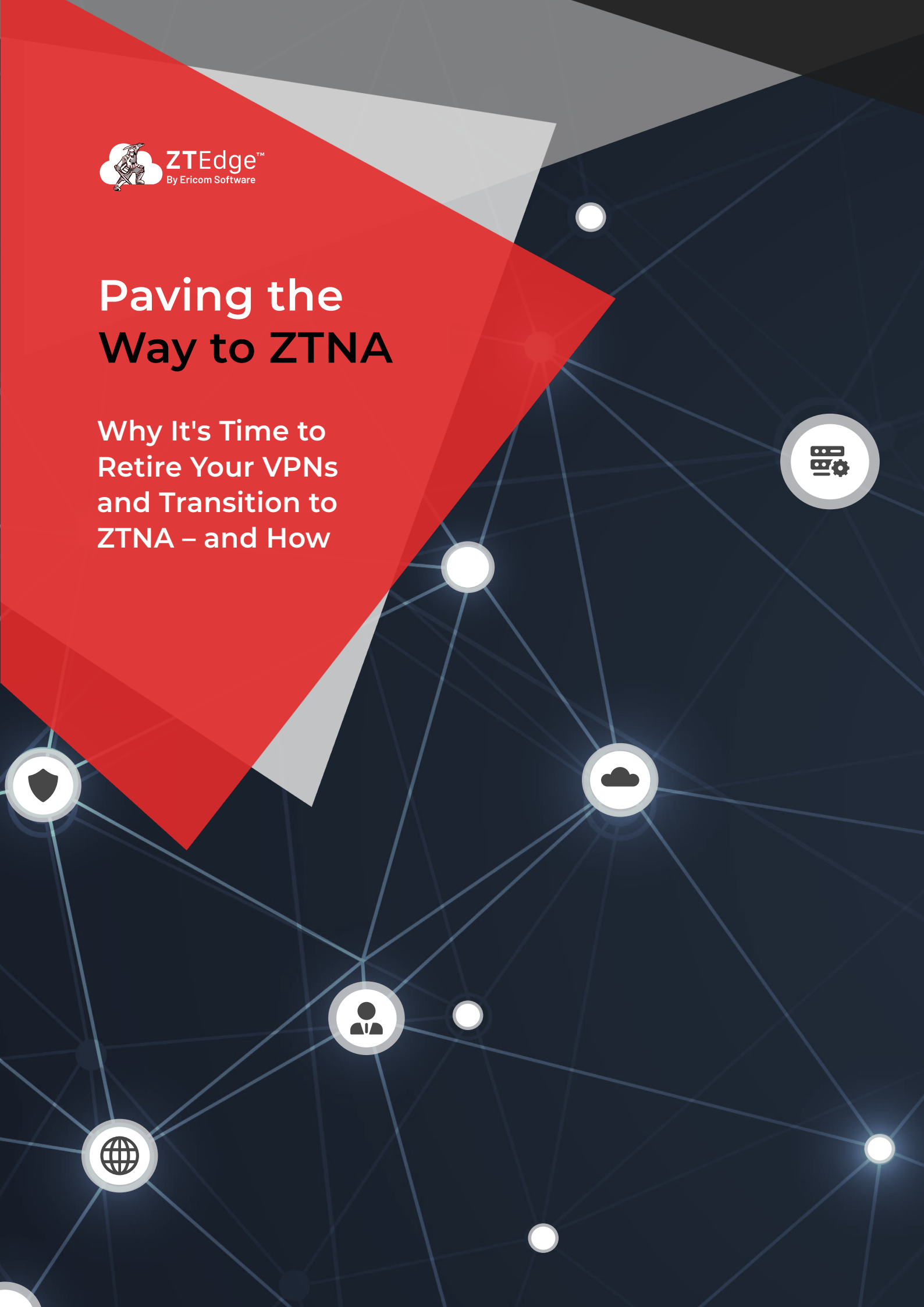
ZTEdge™
By Ericom Software

Paving the Way to ZTNA

Why It's Time to Retire Your VPNs and Transition to ZTNA – and How



Contents

ZTEdge™
By Ericom Software

VPNs: A Solution Whose Time Has Gone

For over a quarter of a century, since their introduction in 1995 as a means to access on-premises datacenters while on the road, VPNs have provided the remote connectivity that businesses depend on.

While VPN protocols have evolved significantly since those early days, with SSL and IPSec protocols added to encrypt data and secure it during transmission, the digital business landscape has changed much more rapidly and profoundly, leaving VPN technology in the dust.

In the rush to enable remote work in the face of pandemic-spurred closures, VPN sales surged. But despite recent investment in VPNs – or more accurately, due to organizations' intense recent experiences with these solutions – it is more clear than ever that there is no time to lose; VPNs must be replaced with more comprehensive, secure and manageable remote access solutions.

There is no time to lose. VPNs must be replaced with comprehensive, secure and manageable remote access solutions.

VPN weaknesses can be divided into three slightly overlapping areas:

The VPN concept

Operational challenges

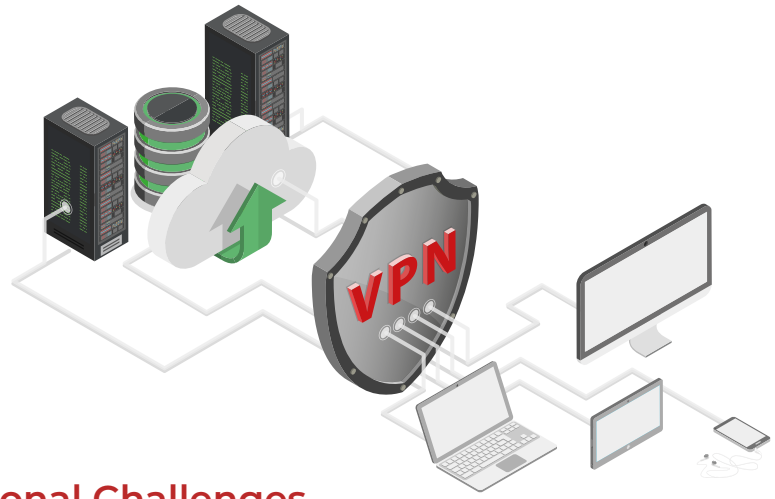
Security issues

ZTEdge™
By Ericom Software

The VPN Concept

Datacenter access is no longer enough

Today, the on-premises datacenters that VPNs were designed to access play a diminishing role in most organizations, as does the software on user devices. Public and private clouds, SaaS apps, and the web are all essential resources that must be accessed securely, but routing access via VPNs to apply security controls is cumbersome and inefficient.



Operational Challenges

VPNs do not play well with others

As legacy technologies designed for a very different computing era, VPNs have poor interoperability with IT, security, and business systems. Because integrations with firewalls and policy management systems is difficult, IT is often faced with difficult choices between installing updates that lead to labor-intensive re-integrations, or risking attack by leaving vulnerabilities unpatched.

Costly and difficult to scale

For decades, VPN capacity was an issue only for the largest organizations with the most mobile workforces. With the imposition of pandemic-related restrictions, however, it became everyone's problem, as organizations worldwide struggled to maintain business continuity. As hardware-based equipment, VPNs have limited capacity and less flexibility. "Scaling" requires additional VPNs must be purchased and installed, which is time-consuming and costly.

Management-intensive

VPNs are typically not centrally managed. Installing and maintaining clients on each user device is a drain on scarce and already over-burdened resources.

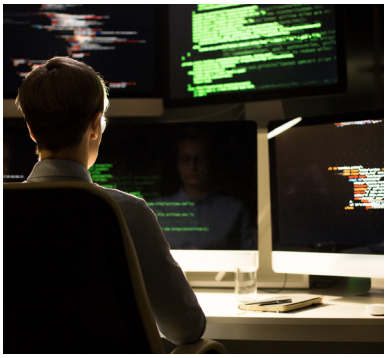
Poor performance

VPN concentrators create chokepoints that can slow down performance, resulting in poor user experience.

ZTEdge™
By Ericom Software

Security Issues

While conceptual and management issues increase VPN costs and reduce their value, security issues associated with VPNs make them downright dangerous and are the most convincing argument for their immediate replacement.



The COVID pandemic drove a sharp increase in VPN use. In the breach, this massive increase in VPN use enabled many businesses to rapidly enable remote work. Unfortunately, it also created vulnerabilities that enabled cybercriminals to hack—or falsely authorize—their way into networks to steal data, deliver malware and launch ransomware attacks.

Weak, non-contextual authentication

VPNs assume a high level of trust, requiring users to provide only a username and password. Since identity is not validated and VPNs lack contextual awareness, logins from unusual or suspicious locations or at odd hours – which more modern solutions would instantly flag as suspicious – are accepted. Successful brute force attacks or attacks via stolen credentials enable additional breaches and malware delivery.

Perimeter-based defense has become obsolete as resources and computing move to the cloud, apps move to the web, and businesses move to remote work.

Broad network access

Another way that VPNs flout Zero Trust principles is by enabling immediate, full tunnel access to entire networks upon connection. As a result, once a user – or cybercriminal – is authorized via the VPN, they have visibility into the full network and can move laterally within to attack any targets.

Open ports

VPN connections are enabled by concentrators, which in turn rely on internet-exposed open ports. Cybercriminals rely on these ports as well, scanning for them and leveraging them as paths to enter target networks.

Software vulnerabilities

VPNs are notoriously prone to software vulnerabilities. Most vendors issue patches immediately upon being notified of vulnerabilities. However, they cannot force customers to apply them. As mentioned above, because patches frequently "break" the delicate integrations between VPNs and other network and security solutions.

ZTEdge™
By Ericom Software

Why Zero Trust is the Right Way to Do Remote Access

The days when "remote access" meant providing access to on-premises databases for on-the-road employees are long gone. Today, users are equally likely – if not more so -- to require access to SaaS and private cloud apps as well as to data, which, of course, may be located on local networks, private clouds or in SaaS apps. As such, the very concept of a VPN, based on access to on-premises networks, is defunct.

"Zero Trust security" seems to be the answer given to virtually every security issue today. And for good reason: By rejecting trust in favor of granular validation and access limitations, it truly lowers risk for organizations that adhere to its concepts.

This is particularly true for remote access. With traditional perimeters gone, the Zero Trust principles of "never trust, always validate," assume breach attack surface reduction and least-privilege access together enable a flexible new breed of personalized perimeters that are unique for each user, software-enforced and – ideally – cloud-based for unlimited reach.

By rejecting trust in favor of granular validation and access limitations, **Zero Trust Security truly lowers risk for organizations** that adhere to its concepts.

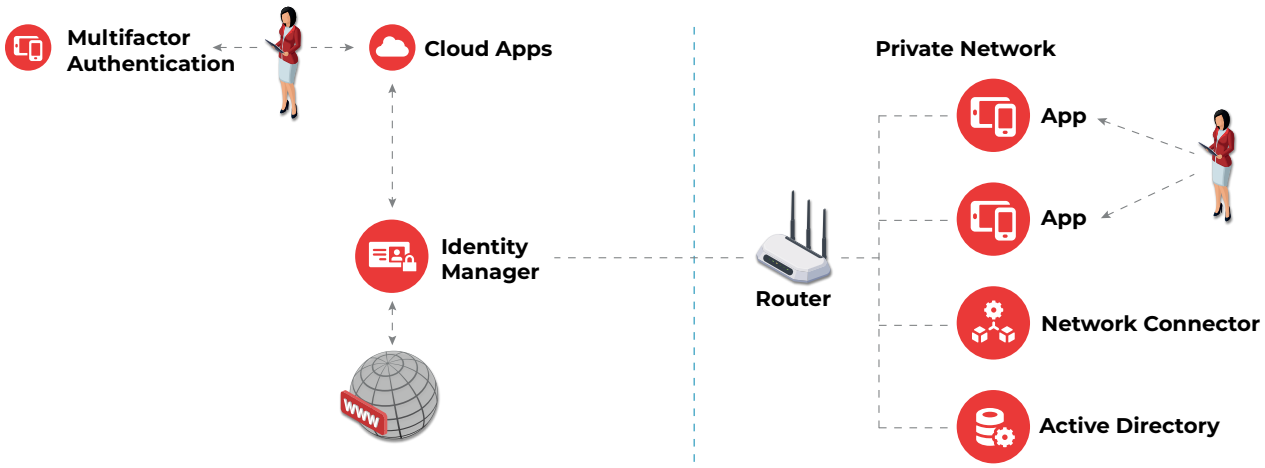
ZTEdge™
By Ericom Software

What's so "Zero Trust" about Zero Trust Network Access (ZTNA)?

Let's look at each of the Zero Trust principles to see how, by adhering to them, ZTNA solutions secure and streamline remote access, eliminate VPN-associated risk, and minimize risk of cyberattacks.

Never trust, always validate

ZTNA solutions leverage strong identity authentication and validation, including multi-factor authentication. They also rely on context-sensitive factors including time, location, device and IP-address. So, for instance, resources that a user might be able to access when they log in from their office or home may not be accessible if they log in at midnight from a bar while on PTO.



Assume breach

While this Zero Trust principle may have, at some point, seemed unduly pessimistic, today we know better. Organizations must do all that they can to keep cybercriminals out but it is equally important – if not more so – to limit damage that can be done if they get in. In network access terms, this means reducing attack surfaces in a number of ways. First, by microsegmenting networks to prevent lateral movement of hackers who manage to gain access, as well as cloaking all resources and apps, so they cannot see what is there to attack.

Least privilege access

VPNs grant users unlimited access to all network resources once they sign in... and grant that same unlimited access to criminals using stolen credentials or brute force attacks to get access. ZTNA leverage granular policies to enforce least-privilege access. So users can access only the resources they need for their work, malicious insiders can do only limited damage, and access is similarly limited for attackers using stolen credentials.

ZTEdge™
By Ericom Software

Not Just More Secure: Flexible, Scalable, Manageable Remote Access

Security, of course, is paramount. However, because any security solution that unduly inconveniences users or is too difficult for IT to manage is doomed to fail, good user practices and easy management are essential as well.

Cloud-based ZTNA solutions are far more flexible, more scalable and more manageable than VPNs. For these reasons and more, ZTNA is also easier and less costly to operate and scale, and less vulnerable to poor management and misuse.

Scalable

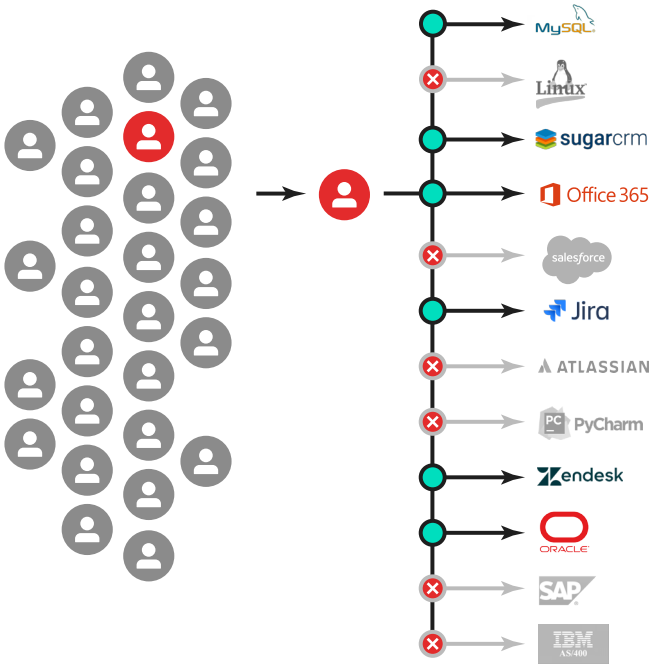
When properly provisioned, cloud-based ZTNA solutions can be dynamically scaled – and then scaled back if it's no longer needed.

Flexible and interoperable

Cloud-based, software-defined ZTNA solutions can be simply and quickly integrated with IT, security and business systems, via APIs. They free organizations to update their infrastructure without VPN compatibility concerns.

Managed through policies

Policies are the secret sauce for your ZTNA solutions – in fact, for all your access security. Strong, granular policies ensure that access is granted only to those who truly need it, for only those resources they truly need. Over-broad policies take the "least" out of least privilege access, exposing resources to wider access and greater risk of attack.



ZTEdge™
By Ericom Software

Convinced? Now What?

So you're on board for ditching your VPNs and moving to ZTNA. But after years – even decades – of VPN use, it's hard to get started. But no worries: We've got you covered.

While hesitancy to implement new solutions is natural, the drumbeat of bad VPN news – including numerous vulnerabilities and exposure of login credentials for 87,000 FortiGate VPNs – is mighty convincing.

In a recent survey, over 80% of respondents indicated that they would start implementing Zero Trust solutions within the next year. A quarter identified network security infrastructure as the top priority to be addressed. For those companies, ZTNA is the natural first step of their transition to Zero Trust.

Upgrading from VPNs to ZTNA in 6 Easy Steps

1

Know where you're coming from

Before you look forward, start by looking back. Understanding who has been using the VPN, how they use it, and what works or does not for them can help you prioritize functionality for ZTNA implementation. Document application usage so you can ensure that access to the most heavily used – and essential – applications is seamless before switching users to ZTNA. Better yet, some ZTNA solutions come with a “learning” function that can observe typical application access patterns and suggest policies to you.

2

Know where you want to go

While ZTNA can certainly be implemented as a stand-alone solution, it requires functionality such as identity and access management (IAM) that is basic to many -- even most – elements encompassed by SASE platforms. Choose a ZTNA solution that integrates easily with your existing network infrastructure, but will also ease your organizations' future Zero Trust implementations. Make sure that the vendor has a strong SASE platform, including a Zero Trust web security offering with remote browser isolation (RBI) and secure web gateway (SWG), as well as a cloud access security broker (CASB) solution.

3

Get help

In a recent survey, over 70% of security & risk professionals indicated that having a qualified partner would accelerate implementation of Zero Trust solutions. This is especially true for ZTNA, since there are a wide variety of solutions available, from companies ranging from tiny start-ups to the largest security solution providers.

Identifying the differentiators and capabilities that are most important for your organization, as well as solutions that will represent the best long-term investment, is a job for knowledgeable security professionals with ZTNA experience.

Consulting a number of professionals can help you decide whether a self-hosted solution is best for your organization, or whether an "as-a-service" ZTNA solution administered by a trusted managed security service provider is a better option.

4

Get your customers on board

Change is hard, especially when the change involves tools that managers, users, customers – and the organization itself – regularly use and depend on. Use what you learned back in Step 1 to identify the most significant points of concern for the different user groups, and work with each to reassure them and show them how ZTNA is going to be easier for them compared to VPNs. For example, explain how ZTNA can both ease the user experience and strengthen security with simpler, context-sensitive authentication.

5

Get your ducks in a row

Strong per-user application access policies and granular microsegmentation are the true powers behind ZTNA access limitations. Take the time to update and rationalize access policies as part of your ZTNA project. Make sure to create policies only for current employees and active third-parties, and include policy expiration dates for contract workers.

As mentioned before, you can save time, money and effort – and get your ZTNA off the ground more quickly – by choosing a solution that leverages machine learning (ML) to automate the initial policy-building process by mapping users to applications, as well as to periodically update privileges based on actual usage.

6

Get going

Time to implement the solution and onboard your users. Ideally, the solution you choose should offer client-based and clientless options. Choose a group of each type of users to implement first, so you can iron out any glitches before implementing more broadly.

7

Fine tune and scale up

Enlist early users in the transition effort through focus groups and questionnaires about their experiences, and apply relevant learnings to the larger roll-out.

Monitor the impact of your VPN-to-ZTNA transition by tracking help desk calls, user satisfaction, and activation of open port and firewall notifications.

Remember that maintaining a true least-privilege stance requires ongoing attention to keeping policies updated. Assign responsibility to IT staff to coordinate with HR and monitor usage, or streamline the process by scheduling ML-based updates, if your solution provides them.

As many organizations' first foray into implementing Zero Trust security, replacing VPNs with Zero Trust Network Access is exciting but also daunting. Careful preparation – including choosing a partner to assist in the process, choosing a solution that meets both immediate and long-term needs, and developing granular policies that allow the organization to reap maximum benefits from the new solution – is the key to a smooth and successful transition.

ZTEdge Remote Application Access is the ideal solution for midsize enterprises and small business that are ready to transition from VPNs to ZTNA. With built-in identity and access management, an automatic policy builder that makes granular policy creation simple, and leading MSSP partners who can free your scarce IT resources from the burden of securing your organization from cyberattack, ZTEdge is the right SASE platform to ease your Zero Trust journey.

Contact us now

www.zerotrustedge.com
info@zerotrustedge.com
US: (201) 767-2210
Europe: +44 (0) 1905 777970
ROW: +972-2-591-1700